There's a Hole in my Container: Docker Security Fix Released

Just in case you missed this news on November 24th, Eric Windisch (@ewindisch) posted an update to the Docker application which answered a couple of vulnerabilities that were present in versions prior to the newly released version 1.3.2 that came out. This highlights the importance of maintaining diligence on watching for vulnerabilities as we run existing tools and integrate new infrastructure components.

The interesting thing when someone said to me "This shows that there may be problems with people using it because this type of thing happens". My response to this was rather simple, and that is to say that every month, Microsoft releases known vulnerability patches on "patch Tuesday", Out-of-band patches are released occasionally also, and if we look across the entire Linux community there are many mailing lists and sites maintaining patch and vulnerability information.

Before I enter soapbox mode, I'll say that you should read the article (http://www.securityfocus.com/archive/1/534082) and then you should ensure that you update your Docker infrastructure accordingly.

Highlights of What this Brings up

Every time there is an announcement of something like this, it is a reminder of a couple of things. Here are my top items that I find become discussion points, and why they are important.

People Think Open Source is Not Completely Secure

This is both true and false. In fact, nothing is "completely secure" if you ask the real security folks and hackers. A completely secure product is just a sign that it hasn't be breached yet, but that at some point there is a very good chance that something could be done to open the doors in one way or another.

The open source model is balked at my many because of the complete availability of the source code which some mistakenly view as giving the keys to the kingdom. What is important about these types of vulnerability notifications is that they are found by community contributors in many cases.

Apple and Microsoft regularly release vulnerability fixes that have been discovered by the community and reported to them. The whitehat hacking movement has been the positive force that has protected many of us as users of these systems. The walled garden has not been the panacea of secure software development as many have touted it to be.

At the same time, being open source is not an automatic path to being secure. In general it can be said that open source has produced very positive responses to security vulnerabilities and continues to be a widely adopted model for that reason.

Is Docker Ready for Prime Time?

This vulnerability is not a reason that Docker isn't ready for deployments on production infrastructure. What may be the hold back on feeling that Docker isn't ready is the that the organizations leveraging it may not have a model that can manage Docker. Running Docker is one thing, but managing it fully is another entire situation. Scaling, deploying, patching, and other

operational management is one of the reasons that some may slow the adoption in their organization. This holds true for any system though and as someone who once ran 350 servers which were patched manually on a monthly basis by a team of operators when I arrived, I know that every system seems like it's not ready for prime time until we put procedures around management in place.

Configuration Management is Needed

This is absolutely true. Every time I am told by someone that they "only have to do something once or twice" I usually find that the once or twice process becomes a production operations procedure and doesn't have proper orchestration wrapped around it to make it truly production ready.

Using configuration management systems like Puppet, System Center Configuration Management (SCCM), Chef and others is very important as we look to answer the call for things like vulnerability management. If you were running Docker already, you could quite neatly use Puppet to deploy updates and bring your environment into compliance.

Patch all the things!

Make sure you patch up your Docker, and keep watching the Docker blog for new releases https://docs.docker.com/release-notes/ to be sure you are staying up to date. Nobody likes a leaky container.